

IRREGULARITIES OF DISTRIBUTION OF DIGITAL (0,1)-SEQUENCES IN PRIME BASE

Henri Faure

*Institut de Mathématiques de Luminy, U.M.R. 6206 CNRS, 163 avenue de Luminy, case 907, F-13288
Marseille Cedex 09, France*

faure@iml.univ-mrs.fr

Received: 1/20/05, Revised: 7/13/05, Accepted: 8/12/05, Published: 9/8/05

Abstract

In this paper, as an application of our recent results to appear elsewhere [5], we compare digital $(0, 1)$ -sequences generated by nonsingular upper triangular matrices in arbitrary prime bases to van der Corput sequences and show these last ones are the worst distributed with respect to the star discrepancy, the extreme discrepancy, the L_2 -discrepancy and the diaphony. Moreover, we obtain digital $(0, 1)$ -sequences in arbitrary prime bases with very good extreme discrepancy, quite comparable to the best generalized van der Corput sequences already found in preceding studies ([2] and [4]).

1. Introduction.

Digital $(0, 1)$ -sequences are one-dimensional coordinate projections of digital $(0, s)$ -sequences [3] which are themselves a special case of digital (t, s) -sequences [10], widely used in multi-dimensional integration in the general setting of quasi-Monte Carlo methods. While multi-dimensional sequences are difficult to handle—the order of their discrepancy is still unknown—the one-dimensional case is much more tractable and precise results are available. Their interest is twofold, number theoretical (better knowledge of irregularities of distribution) and practical (improvement and acceleration of quasi-Monte Carlo methods by scrambling techniques).

Motivated by these two facets, recent researches on digital sequences have been achieved in base 2 ([9], [11] and others under publication by the same authors), following a previous, but less informative, study in larger bases [7]. Then in [5], we have obtained exact formulas for the discrepancies and the diaphony of a wide class of digital sequences in arbitrary prime bases, the NUT digital $(0, 1)$ -sequences (see Section 3 for

the definition); and next, from these formulas, we have deduced selection criteria for the scrambling of multi-dimensional digital sequences by a classification of the digits involved in their construction [6].

Our purpose in the present article is to compare the irregularities of distribution of NUT digital $(0, 1)$ -sequences with those of generalized van der Corput sequences, especially the best ones. First (Section 5.1), we show that the original van der Corput sequences are the worst distributed among the NUT digital $(0, 1)$ -sequences in prime base, with respect to the four measures D , D^* , T and F (see Section 2); the proof for the diaphony requires a deep analysis of the related key function χ (Lemma 3). Then (Section 5.2), we compare the best NUT digital $(0, 1)$ -sequences with very good generalized van der Corput sequences by means of the classical quality parameter for the extreme discrepancy of these sequences. The simplicity of the formula for the extreme discrepancy of NUT digital $(0, 1)$ -sequences permits computations for very large bases and is promising for finding new very low discrepancy sequences. At the present, we cannot say anything about general $(0, 1)$ -sequences which are not NUT digital ones.

Sections 2 and 3 contain basic definitions and Section 4 states the fundamental results of [5] we need for our comparative study.

2. Irregularities of Distribution.

Let $X = (x_n)_{n \geq 1}$ be an infinite sequence in $[0, 1]$, $N \geq 1$ an integer and $[\alpha, \beta[$ a subinterval of $[0, 1]$; the *error* to ideal distribution is the difference

$$E([\alpha, \beta[; N; X) = A([\alpha, \beta[; N; X) - Nl([\alpha, \beta[$$

where $A([\alpha, \beta[; N; X)$ is the number of indices n such that $1 \leq n \leq N$ and $x_n \in [\alpha, \beta[$ and where $l([\alpha, \beta[$ is the length of $[\alpha, \beta[$.

To avoid any ambiguity, recall that $[\alpha, \beta[= [0, \beta[\cup [\alpha, 1[$ if $\alpha > \beta$ ([1], p.105), so that $l([\alpha, \beta[) = 1 - \alpha + \beta$ and $E([\alpha, \beta[; k; X) = -E([\beta, \alpha[; k; X)$.

Definition of the *extreme discrepancies*:

$$D(N, X) = \sup_{0 \leq \alpha < \beta \leq 1} |E([\alpha, \beta[; N; X)|,$$

$$D^*(N, X) = \sup_{0 \leq \alpha \leq 1} |E([0, \alpha[; N; X)|,$$

$$D^+(N, X) = \sup_{0 \leq \alpha \leq 1} E([0, \alpha[; N; X),$$

$$D^-(N, X) = \sup_{0 \leq \alpha \leq 1} (-E([0, \alpha[; N; X)).$$

Usually, D is called the extreme discrepancy and D^* the star discrepancy; D^+ and D^- are linked to the preceding one's by

$$D(N, X) = D^+(N, X) + D^-(N, X) \text{ and } D^*(N, X) = \max(D^+(N, X), D^-(N, X)).$$

Definition of the L_2 -discrepancy and of the diaphony:

$$T(N, X) = \left(\int_0^1 (E([0, \alpha[; N; X])^2 d\alpha \right)^{\frac{1}{2}},$$

$$F(N, X) = \left(2 \sum_{m=1}^{\infty} \frac{1}{m^2} \left| \sum_{n=1}^N \exp(2i\pi m x_n) \right|^2 \right)^{\frac{1}{2}}.$$

The diaphony F and the L_2 -discrepancy T are related by the formula of Koksma ([8], Lemma 2.8)

$$T^2(N, X) = \left(\sum_{n=1}^N \left(\frac{1}{2} - x_n \right) \right)^2 + \frac{1}{4\pi^2} F^2(N, X).$$

3. Digital (0,1)-Sequences and Related Functions.

In this section, we define the class of digital (0, 1)-sequences we are concerned with and we recall the definition of generalized van der Corput sequences [2], the two families being closely related; then we introduce a set of functions which are the key tools for the study of both families. Let $b \geq 2$ be a prime number.

For integers n and N with $n \geq 1$ and $1 \leq N \leq b^n$, write $N - 1 = \sum_{r=0}^{\infty} a_r(N) b^r$ in the b -adic system, so that $a_r(N) = 0$ if $r \geq n$.

The *digital (0, 1)-sequences* in prime base b we consider can be simply described as follows:

$$X_b^C = (x_N)_{N \geq 1}, \quad \text{with } x_N = \sum_{r=0}^{\infty} \frac{x_{N,r}}{b^{r+1}} \text{ in which } x_{N,r} = \sum_{k=r}^{\infty} c_r^k a_k(N) \pmod{b},$$

the generator matrix $C = (c_r^k)_{r \geq 0, k \geq 0}$ being an infinite *nonsingular upper triangular* (NUT) matrix with entries $c_r^k \in \mathbb{F}_b$ identified as a set to $\{0, 1, \dots, b - 1\}$.

From the definitions of the $a_k(N)$ and of C , the summations above are finite. In brief, we name these sequences *NUT digital (0, 1)-sequences*.

Let $\Sigma = (\sigma_r)_{r \geq 0}$ be a sequence of permutations of \mathbb{F}_b . The *generalized van der Corput sequence* S_b^Σ in base b associated with Σ is defined by

$$S_b^\Sigma(N) = \sum_{r=0}^{\infty} \frac{\sigma_r(a_r(N))}{b^{r+1}}.$$

Note that if the generator matrix C is diagonal we have $X_b^C = S_b^\Delta$, where $\Delta = (\delta_r)_{r \geq 0}$ is the sequence of permutations of \mathbb{F}_b defined by $\delta_r(i) = c_r^x i \pmod{b}$, i.e. δ_r is the multiplication in \mathbb{F}_b by the diagonal entry c_r^x . Now, if C is not diagonal, as we shall see in the next section, the diagonal entries will still determine the same permutations δ_r , but the exact formulas for D^+ , D^- , D^* and T will involve translated permutations (depending on $N \geq 1$) of the δ_r 's; on the contrary, and surprisingly, D and F will only depend on the δ_r 's.

Functions $\varphi_{b,h}^\sigma$ related to a pair (b, σ) .

Let σ be a permutation of \mathbb{F}_b and set $Z_b^\sigma := \left(\frac{\sigma(0)}{b}, \dots, \frac{\sigma(b-1)}{b}\right)$. For any integer h with $0 \leq h \leq b-1$, the real function $\varphi_{b,h}^\sigma$ is defined as follows:

Let k be an integer with $1 \leq k \leq b$; then for every $x \in \left[\frac{k-1}{b}, \frac{k}{b}\right[$ we set:

$$\varphi_{b,h}^\sigma(x) = A\left(\left[0, \frac{h}{b}\right[; k; Z_b^\sigma\right) - hx \quad \text{if } 0 \leq h \leq \sigma(k-1) \quad \text{and}$$

$$\varphi_{b,h}^\sigma(x) = (b-h)x - A\left(\left[\frac{h}{b}, 1\right[; k; Z_b^\sigma\right) \quad \text{if } \sigma(k-1) < h < b;$$

finally the function $\varphi_{b,h}^\sigma$ is extended to the reals by periodicity. Note that $\varphi_{b,0}^\sigma = 0$.

In the very special case $b = 2$, we only have two permutations which give either $\varphi_{2,1}^\sigma = \|\cdot\|$, if σ is the identical permutation or $\varphi_{2,1}^\sigma = -\|\cdot\|$, if $\sigma = (0\ 1)$, where $\|\cdot\|$ is the distance to the nearest integer function.

Actually, the b functions $\varphi_{b,h}^\sigma$ give rise to other functions, depending only on (b, σ) , according to the involved notion of discrepancy: for the extreme discrepancies

$$\psi_b^{\sigma,+} = \max_{0 \leq h \leq b-1} (\varphi_{b,h}^\sigma), \quad \psi_b^{\sigma,-} = \max_{0 \leq h \leq b-1} (-\varphi_{b,h}^\sigma) \quad \text{and} \quad \psi_b^\sigma = \psi_b^{\sigma,+} + \psi_b^{\sigma,-}$$

and for the L_2 -discrepancy and the diaphony

$$\varphi_b^\sigma = \sum_{h=0}^{b-1} \varphi_{b,h}^\sigma, \quad \phi_b^\sigma = \sum_{h=0}^{b-1} (\varphi_{b,h}^\sigma)^2 \quad \text{and} \quad \chi_b^\sigma = b\phi_b^\sigma - (\varphi_b^\sigma)^2.$$

With the help of these functions, we are able to obtain exact formulas for the discrepancies and the diaphony of NUT digital $(0, 1)$ -sequences, as we did for the generalized van der Corput sequences [1], [2].

4. Exact Formulas for NUT Digital (0,1)-Sequences.

We present here the formulas for the NUT digital (0, 1)-sequences we shall use in the two next sections (these results come from our paper [5]). For this purpose, we need a further definition: we use the symbol \uplus to denote the translated permutation of a given permutation σ of \mathbb{F}_b by an element $t \in \mathbb{F}_b$ in the following sense

$$(\sigma \uplus t)(i) := \sigma(i) + t \pmod{b} \quad \text{for all } i \in \mathbb{F}_b.$$

Moreover, associated with the NUT generator matrix $C = (c_r^k)_{r \geq 0, k \geq 0}$, we recall the permutation δ_r defined by $\delta_r(i) := c_r^r i \pmod{b}$ and we introduce the quantity

$$\theta_r(N) := \sum_{k=r+1}^{\infty} c_r^k a_k(N) \pmod{b},$$

where the $a_k(N)$'s are the digits of $N-1$. Note that $a_k(N) = 0$ for all $k \geq n$ if $1 \leq N \leq b^n$, thus $\theta_r(N) = 0$ and $\sigma_r = \delta_r$ for all $r \geq n-1$ in this case. This quantity determine the translated permutations which appear in the formulas for D^+, D^-, D^* and T .

We are now in a position to state our results:

Theorem 1. *For all integers n and N with $1 \leq N \leq b^n$, we have*

$$\begin{aligned} D^+(N, X_b^C) &= \sum_{j=1}^n \psi_b^{\delta_{j-1} \uplus \theta_{j-1}(N), +} \left(\frac{N}{b^j} \right) + \frac{N}{b^n}, \\ D^-(N, X_b^C) &= \sum_{j=1}^n \psi_b^{\delta_{j-1} \uplus \theta_{j-1}(N), -} \left(\frac{N}{b^j} \right), \\ D(N, X_b^C) &= \sum_{j=1}^n \psi_b^{\delta_{j-1}} \left(\frac{N}{b^j} \right) + \frac{N}{b^n}, \\ \frac{1}{4\pi^2} F^2(N, X_b^C) &= \frac{1}{b^2} \sum_{j=1}^n \chi_b^{\delta_{j-1}} \left(\frac{N}{b^j} \right) + \frac{N^2}{12 b^{2n}} \quad \text{and} \\ T^2(N, X_b^C) &= \left(\frac{1}{b} \sum_{j=1}^n \varphi_b^{\delta_{j-1} \uplus \theta_{j-1}(N)} \left(\frac{N}{b^j} \right) + \frac{N}{2b^n} \right)^2 + \frac{1}{b^2} \sum_{j=1}^n \chi_b^{\delta_{j-1}} \left(\frac{N}{b^j} \right) + \frac{N^2}{12 b^{2n}}. \end{aligned}$$

Remarks. 1. As already noted in the preceding section, we see from the formulas for D and F that digital (0,1)-sequences generated by NUT matrices having the same diagonal have the same extreme discrepancy and the same diaphony. Therefore, for these two measures of Irregularities of Distribution, generalized van der Corput sequences and NUT digital (0, 1)-sequences have the same behaviour, provided that, for the last ones,

we consider the sequence of permutations Δ resulting from the multiplications in \mathbb{F}_b by the diagonal entries of C : $D(N, X_b^C) = D(N, S_b^\Delta)$ and $F(N, X_b^C) = F(N, S_b^\Delta)$.

2. As for D^+ , D^- , D^* and T , the formulas are similar to those for the generalized van der Corput sequences, but the situation is more complicated because of the quantity $\theta_{j-1}(N)$ which depends on N , via the b -adic expansion of $N - 1$, and on the NUT generator matrix C , via its entries strictly above the diagonal. Very few results have been available and only in base 2 ([9] and [11]), except loose bounds in a special case for T ([7]). In arbitrary prime bases, we shall obtain general bounds in Section 5; but sharp results on D^* and T will need further investigations.

3. For the L_2 -discrepancy, according to the behaviour of the diaphony (its order is $O(\sqrt{\log N})$, see [1] Theorem 4.6 with $b_j = b$), we have

$$T^2(N, X_b^C) = \frac{1}{b^2} \left(\sum_{j=1}^{\infty} \varphi_b^{\delta_{j-1} \uplus \theta_{j-1}(N)} \left(\frac{N}{b^j} \right) \right)^2 + O(\log N).$$

Therefore the behaviour of the L_2 -discrepancy of X_b^C depends only on the properties of

the functions $\varphi_b^\sigma = \sum_{h=0}^{b-1} \varphi_{b,h}^\sigma$.

5. Comparing NUT Digital (0,1)-Sequences and van der Corput Sequences.

In this section, we first compare NUT digital (0,1)-sequences in prime base b with the original van der Corput sequences, i.e. $S_b^I = X_b^I$ (in which I is either the identical permutation or the identity matrix) and show that the last ones are the worst distributed for D^* , D , T and F . Then we give the results of computational investigations of good NUT digital (0,1)-sequences with respect to D and compare with the best known generalized van der Corput sequences.

5.1 NUT sequences towards van der Corput sequences.

Theorem 2. *For all integers n and N with $1 \leq N \leq b^n$, we have*

$$\begin{aligned} D^*(N, X_b^C) &\leq D(N, X_b^C) \leq D^*(N, S_b^I) = D(N, S_b^I) \\ T(N, X_b^C) &\leq T(N, S_b^I) \\ F(N, X_b^C) &\leq F(N, S_b^I). \end{aligned}$$

Proof. This theorem is an immediate consequence of the three following lemmas together with Theorem 1. ◇

Remark. From our preceding studies, [2] Theorem 6 and [1] Theorems 4.12 and 4.13, the exact asymptotic behaviour of $D(N, S_b^I)$, $T(N, S_b^I)$ and $F(N, S_b^I)$ is already known.

Lemma 1. For any permutation σ of \mathbb{F}_b , we have the inequality $\psi_b^\sigma \leq \psi_b^I$.

Proof. See the proof of Corollary 3, 5.5.4 p.180 [2]. ◇

Lemma 2. For any permutation σ of \mathbb{F}_b , we have the inequality $|\varphi_b^\sigma| \leq \varphi_b^I$.

Proof. Let us first recall the main property of the functions φ_b^σ ([1], Property 3.5 (i), p.109), where f' is the right derivative of f :

$$(\varphi_b^\sigma)'(\frac{k}{b}) = \frac{b(b-1)}{2} - b\sigma(k) \quad \text{for } 0 \leq k \leq b-1, \quad \text{so that} \quad \varphi_b^\sigma(\frac{k}{b}) = \frac{1}{b} \sum_{j=0}^{k-1} (\varphi_b^\sigma)'(\frac{j}{b}).$$

Therefore, the derivatives of φ_b^σ on $[0, 1]$ take once only the values $jb - \frac{b(b-1)}{2}$ for $0 \leq j \leq b-1$.

Now, to get a permutation maximizing $|\varphi_b^\sigma|$, it is sufficient to take the derivatives in the order

$$\frac{b(b-1)}{2}, \frac{b(b-1)}{2} - b, \dots, b, 0, -b, \dots, -\frac{b(b-1)}{2}$$

on the intervals $[\frac{j}{b}, \frac{j+1}{b}]$ for $0 \leq j \leq b-1$. As a matter of fact, this procedure gives exactly the identical permutation (the other possibility should be to take the derivatives in the opposite order, in which case we should get $-\varphi_b^I = \varphi_b^J$, the permutation J being defined by $J(k) = b-1-k$). ◇

Lemma 3. For any permutation σ of \mathbb{F}_b , we have the inequality $\chi_b^\sigma \leq \chi_b^I$.

Proof. This inequality requires more attention than the previous ones.

First, recall that ([1], Definition 3.4)

$$\chi_b^\sigma = b\phi_b^\sigma - (\varphi_b^\sigma)^2 = \sum_{0 \leq h < h' < b} (\varphi_{b,h'}^\sigma - \varphi_{b,h}^\sigma)^2 = \frac{1}{2} \sum_{h \neq h'} (\varphi_{b,h'}^\sigma - \varphi_{b,h}^\sigma)^2$$

and that ([1], Property 3.5 (ii)) on each interval $[\frac{k-1}{b}, \frac{k}{b}]$ ($1 \leq k \leq b$), χ_b^σ has the form $\chi_b^\sigma(x) = \frac{b^2(b^2-1)}{12}x^2 + Ax + B$ with A and B depending on σ and k ; thus $\chi_b^I - \chi_b^\sigma$ is an affine function, so that $\chi_b^I - \chi_b^\sigma \geq 0$ if and only if $\chi_b^I(\frac{k}{b}) \geq \chi_b^\sigma(\frac{k}{b})$ for all $1 \leq k \leq b$.

On the other hand, for arbitrary $h \neq h'$, $\varphi_{b,h'}^\sigma(\frac{k}{b}) - \varphi_{b,h}^\sigma(\frac{k}{b}) = E([\frac{h}{b}, \frac{h'}{b}]; k; Z_b^\sigma)$ since $\varphi_{b,h}^\sigma(\frac{k}{b}) = E([0, \frac{h}{b}]; k; Z_b^\sigma)$ (see [2], proof of Property 3.2.2 (a) or [5], proof of the proposition of section 6.6). Therefore, proving Lemma 3 amounts to proving that for fixed k ($1 \leq k \leq b$)

$$\sum_{h \neq h'} \left(E([\frac{h}{b}, \frac{h'}{b}]; k; Z_b^\sigma) \right)^2 \leq \sum_{h \neq h'} \left(E([\frac{h}{b}, \frac{h'}{b}]; k; Z_b^I) \right)^2.$$

To obtain this result, we split up the sum into sets of couples (h, h') satisfying $l([\frac{h}{b}, \frac{h'}{b}]) = \frac{d}{b}$, with $1 \leq d \leq b - 1$, so that we get $(b - 1)$ sets, each one containing b terms, and we proceed to compare the two sums set by set with fixed d .

In other words, we take a window $(\frac{d}{b})$ -wide and we move the window along the torus $[0, 1[$ with the step $\frac{1}{b}$ (from $[0, \frac{d}{b}[$, $[\frac{1}{b}, \frac{d+1}{b}[$, and so on until $[1 - \frac{1}{b}, \frac{d-1}{b}[$), calculating at each step the remainder

$$E([\frac{h}{b}, \frac{h'}{b}]; k; Z_b^\sigma) = \delta_{h,h'}^\sigma - \frac{dk}{b} \quad \text{with} \quad \delta_{h,h'}^\sigma := A([\frac{h}{b}, \frac{h'}{b}]; k; Z_b^\sigma)$$

and summing the squares.

In that way, we get $l(h, h') = d$ stands for $l([\frac{h}{b}, \frac{h'}{b}]) = \frac{d}{b}$

$$\sum_{l(h,h')=d} (\delta_{h,h'}^\sigma - \frac{dk}{b})^2 = \sum_{l(h,h')=d} (\delta_{h,h'}^\sigma)^2 - \frac{2dk}{b} \sum_{l(h,h')=d} \delta_{h,h'}^\sigma + \frac{d^2k^2}{b^2} \sum_{l(h,h')=d} 1.$$

Now, we claim that $\sum_{l(h,h')=d} \delta_{h,h'}^\sigma = kd$, whatever σ may be: indeed, we have k points of

Z_b^σ and each one occurs d times in $A([\frac{h}{b}, \frac{h'}{b}]; k; Z_b^\sigma) = \delta_{h,h'}^\sigma$ when the window moves from $[0, \frac{d}{b}[$ to $[1 - \frac{1}{b}, \frac{d-1}{b}[$. Thus we obtain

$$\sum_{l(h,h')=d} (\delta_{h,h'}^\sigma - \frac{dk}{b})^2 = \sum_{l(h,h')=d} (\delta_{h,h'}^\sigma)^2 - \frac{d^2k^2}{b} \quad \text{for any } \sigma,$$

so that, to prove Lemma 3, we need only to compare $\sum_{l(h,h')=d} (\delta_{h,h'}^\sigma)^2$ to $\sum_{l(h,h')=d} (\delta_{h,h'}^I)^2$ with

the condition $\sum_{l(h,h')=d} \delta_{h,h'}^\sigma = \sum_{l(h,h')=d} \delta_{h,h'}^I = kd$.

Since, from the definition of $\delta_{h,h'}^\sigma$ we have $0 \leq \delta_{h,h'}^\sigma \leq \min(k, d)$, we must distinguish two cases: $d \leq k$ and $d \geq k$.

Consider first $d \leq k$. It is easy to compute the $(\delta_{h,h'}^I)$'s: $\delta_{h,h+d}^I = d$ for $0 \leq h \leq k - d$, then $\delta_{k-d+j,k+j}^I = d - j$ for $1 \leq j \leq d - 1$, then $\delta_{h,h+d}^I = 0$ for $k \leq h \leq b - d$ and finally $\delta_{b-d+j,j}^I = j$ for $1 \leq j \leq d - 1$, assuming that $k + d \leq b$; otherwise, the smaller values do not exist (no 0 if $k + d = b + 1$, no 0 and no 1 if $k + d = b + 2$ and so on).

Moreover, we note that these values are also obtained for the permutations σ for which the first k points of Z_b^σ are concentrated on an interval of length $\frac{k}{b}$. And as soon as this condition is not realized, the maximal value d for the $(\delta_{h,h'}^I)$'s is obtained less than $(k - d + 1)$ times, compensated by other δ 's since $\sum_{l(h,h')=d} \delta_{h,h'}^\sigma = kd$ is constant.

Therefore, we have to deal with the following optimization problem: in the b -dimensional space \mathbb{R}^b , find the maximal distance to the origin of a point $(x_i) \in \mathbb{Z}^b$ satisfying the

conditions: $0 \leq x_i \leq d$, $\sum_{i=1}^b x_i = kd$ ($1 \leq d \leq k \leq b$) and $x_i = d$ for at most $(k - d + 1)$ indices i . Clearly, the maximum is attained when (x_i) belongs to a lower dimensional hyperface of the hypercube $[0, d]^b$, i.e. when $x_i = d$ for $(k - d + 1)$ indices i ; and that corresponds (among others) to the identical permutation whatever k may be between 1 and b . So, we have proved that $\sum_{l(h,h')=d} (\delta_{h,h'}^\sigma)^2 \leq \sum_{l(h,h')=d} (\delta_{h,h'}^I)^2$ in the case $d \leq k$.

In the second case, $d \geq k$, we proceed in the same way, but here $\delta_{h,h'}^\sigma$ is at most equal to k and at most $(d - k + 1)$ times, which situation again corresponds to permutations σ such that the first k points of Z_b^σ are concentrated on an interval of length $\frac{k}{b}$, in particular the identical permutation. The optimization problem is the same, with the hypercube $[0, k]^b$ instead of $[0, d]^b$ and the maximal distance to the origin is reached when $x_i = k$ for the maximal number $(d - k + 1)$ of indices i , that is, as to our problem, when σ is the identical permutation. This second case completes the proof of Lemma 3. \diamond

Remark. The proofs of Lemma 2 and 3 should be the same for an arbitrary integer, odd or even. Therefore, we can assert that Theorem 2 is also valid for generalized van der Corput sequences in any base (for D and D^* , it is already in [2], 5.5.4 Corollary 3):

$$D^*(N, S_b^\Sigma) \leq D(N, S_b^\Sigma) \leq D^*(N, S_b^I) = D(N, S_b^I),$$

$$T(N, S_b^\Sigma) \leq T(N, S_b^I) \quad \text{and} \quad F(N, S_b^\Sigma) \leq F(N, S_b^I).$$

5.2 NUT sequences towards generalized van der Corput sequences.

In this subsection, we compare the extreme discrepancy of digital $(0, 1)$ -sequences generated by NUT matrices C with $c_r^r = f$ to generalized van der Corput sequences by means of good permutations. For this purpose, we recall formulas giving the asymptotic behaviour of the extreme discrepancy of these sequences (see [2] Theorem 2, Property 3.2.2 and Lemma 4.2.2):

Set $d_b^\sigma(n) = \sup_{x \in [0,1]} \sum_{j=1}^n \psi_b^\sigma(\frac{x}{b^j})$ and $\alpha_b^\sigma = \inf_{n \geq 1} \frac{d_b^\sigma(n)}{n}$. Then $\limsup_{N \rightarrow \infty} \frac{D(N, S_b^\sigma)}{\log N} = \frac{\alpha_b^\sigma}{\log b}$

and

$$D(N, S_b^\sigma) \leq \frac{\alpha_b^\sigma}{\log b} \log N + \alpha_b^\sigma + 2 \quad \text{for all } N \geq 1 \quad (\text{Theorem 2}).$$

Moreover, $\alpha_b^\sigma = \lim_{n \rightarrow \infty} \frac{d_b^\sigma(n)}{n}$ and there exists β_n with $0 \leq \beta_n \leq 1$ such that

$$d_b^\sigma(n) = \alpha_b^\sigma n + \beta_n, \quad \text{so that } 0 \leq d_b^\sigma(1) - \alpha_b^\sigma \leq 1 \quad (\text{Lemma 4.2.2}).$$

Therefore, the quality parameter α_b^σ may be approached with a good approximation by $d_b^\sigma(1)$, that is by computing the quantity

$$d_b^\sigma := \max_{1 \leq k \leq b} \max_{0 \leq h' < h < b} |E([h'/b, h/b]; k; Z_b^\sigma)|$$

since $d_b^\sigma = \sup_{x \in [0,1]} \psi_b^\sigma(x) = d_b^\sigma(1)$ (Property 3.2.2 (ii)).

The interest is that d_b^σ is easy to compute while other approaches of α_b^σ should need to make explicit the huge function ψ_b^σ . We have already performed a program to compute d_b^f (where f refers to the permutation resulting from the multiplication by f) in order to obtain the numerical results which are going to appear in [6]. Here, we make use of it to get the best factors f for arbitrary prime bases. The results are given in the following Table 1 together with the identical permutation I , the permutations σ from [4] and the best permutations σ_0 we have found in our preceding studies.

Comments. For decimal numbers, we have kept the first two digits only.

The bases 12 and 36 give the smallest discrepancies currently known, see [4].

We have computed the best factors f up to $b=1301$. The bases 89 and 233 give the best constants for $2 \leq b \leq 863$ and 233 the best in all. Among the 212 prime numbers considered, few constants are above 0.5, mainly for small b . Recall that $\alpha_2^I = 1/3$ so that $\frac{\alpha_2^I}{\log 2} \approx 0.48$ and $\alpha_3^I = 1/2$ so that $\frac{\alpha_3^I}{\log 3} \approx 0.45$; therefore, we see that our best factors give often better bounds than the exact asymptotic constants for bases 2 and 3. Prospecting permutations for bases close or equal to 89 or 233 for instance should give very low discrepancy sequences.

Acknowledgements.

We would like to thank warmly the organisers of the meeting of Strobl for their efficiency and their hospitality, especially Gerhard Larcher who supported also our visit to Linz just after the conference.

References

- [1] Chaix, H., Faure, H.: Discr panance et diaphonie en dimension un. Acta Arith., **63.2**, 103–141 (1993).
- [2] Faure, H.: Discr panance de suites associ es   un syst me de num ration (en dimension un). Bull. Soc. math. France, **109**, 143–182 (1981).
- [3] Faure, H.: Discr panance de suites associ es   un syst me de num ration (en dimension s). Acta Arith., **41**, 337–351 (1982).

Table 1: Comparisons

base	bd_b^I	bd_b^σ	$bd_b^{\sigma_0}$	fact f	bd_b^f	$\frac{d_b^I}{\log b}$	$\frac{d_b^\sigma}{\log b}$	$\frac{d_b^{\sigma_0}}{\log b}$	$\frac{d_b^f}{\log b}$
2	1	1	1	1	1	0.72	0.72	0.72	0.72
3	2	2	2	1	2	0.60	0.60	0.60	0.60
5	6	4	4	2	4	0.74	0.49	0.49	0.49
7	12	8	6	2	8	0.88	0.58	0.44	0.58
11	30	13	13	3	14	1.13	0.49	0.49	0.53
12	36	16	12	–	–	1.20	0.53	0.40	–
13	42	19	15	5	16	1.25	0.56	0.44	0.47
17	72	26	21	5	28	1.49	0.53	0.43	0.58
19	90	27	25	7	28	1.60	0.48	0.44	0.50
23	132	–	–	5	40	1.83	–	–	0.55
29	210	–	–	8	50	2.15	–	–	0.51
31	240	67	–	12	52	2.25	0.62	–	0.48
36	324	60	51	–	–	2.51	0.46	0.39	–
37	342	–	–	8	72	2.55	–	–	0.53
89	1980	–	–	34	180	4.95	–	–	0.45
233	13572	–	–	89	564	10.68	–	–	0.44

- [4] Faure, H.: Good permutations for extreme discrepancy. *J. Number Theory*, **41**, 47–56 (1992).
- [5] Faure, H.: Discrepancy and diaphony of digital (0,1)-sequences in prime base. *Acta Arith.*, **117.2**, 125–148 (2005).
- [6] Faure, H.: Selection criteria for (random) generation of digital (0,1)-sequences. In: Niederreiter, H., Talay, D. (eds) *Monte Carlo and Quasi-Monte Carlo Methods 2004*. Springer, Berlin Heidelberg New York (to appear).
- [7] Grozdanov, V.S.: On the diaphony of one class of one-dimensional sequences. *Int. J. Math. and Math. Sci.*, **19.1**, 115–124 (1996).
- [8] Kuipers, L., Niederreiter, H.: *Uniform Distribution of Sequences*. Wiley, New York (1974).
- [9] Larcher, G., Pillichshammer F.: Sums of distances to the nearest integer and the discrepancy of digital nets. *Acta Arith.*, **106.4**, 379–408 (2003).
- [10] Niederreiter, H.: *Random Number Generation and Quasi-Monte Carlo Methods*. CBMS-NSF Regional Conference Series in Applied Mathematics. SIAM, Philadelphia (1992).
- [11] Pillichshammer, F.: On the discrepancy of (0,1)-sequences. *J. Number Theory*, **104**, 301–314 (2004).